# EXHIBIT 14

**UNITED STATES DISTRICT COURT**

**FOR THE NORTHERN DISTRICT OF CALIFORNIA**

Case No. 13-cv-04545-JST

***TVIIM, LLC V. McAfee, INC.***

EXPERT REPORT OF DR. MOSES GARUBA

PURSUANT TO FEDERAL RULE OF CIVIL PROCEDURE 26(a)(2)(B)

January 16, 2015

**HIGHLY CONFIDENTIAL**

**ATTORNEYS' EYES ONLY**

formal training and experience. Hacking and hackers, while not unique to the computer security industry, are synonymous in the computer security industry as gaining knowledge in computer security outside of, or as a supplement to formal education. It is not uncommon for recognized experts in computer security to lack a formal degree from a university. For this reason, I would not limit knowledge in the art of computer security at this time to someone with a formal degree in computer programming or computer security. Practical experience with computer security, and in particular, programing a computer security system, would be of equal if not greater value at this time to gain knowledge and skill in the art of computer security at this time. For this reason, I would define someone with skill in the art of computer security as someone with at least a bachelor's degree in computer science with an emphasis in computer security and at least one year of direct practical experience in computer security engineering, or five or more years of direct practical experience in computer security engineering.

**3. Relevant Claims of the '168 Patent**

I understand that there are 9 claims at issue in this case. There are two independent claims, Claims 1 and 11. Five claims are dependent claims of Claim 1, Claims 2, 3, 7, 8, and 9. Three claims are dependent claims of Claim 11, Claims 12, 19 and 20. Claim 1 and its dependent claims are apparatus claims. Claim 11 and its dependent claims are method claims.

**a) Claim 1**

A security system for a computer apparatus, wherein said computer apparatus includes a processor and system memory, said security system comprising:

> at least one security module which under direction from the processor accesses and analyzes selected portions of the computer apparatus to identify vulnerabilities;

identifies whether there are any [redacted]

- "at least one utility module" The Vulnerability Scanner identifies the availability of patches or updates for programs, including those with identified vulnerabilities, and download such patches or updates to the computer apparatus. If an update is found, that information is presented to the user and/or the update is installed.
- "which under the direction from the processor, performs various utility functions with regards to the computer apparatus" The Vulnerability Scanner identifies availability of a patch, accesses and downloads that patch, and installs the same on the computer system.
- "in response to the identified vulnerabilities;" [redacted] the Vulnerability Scanner identifies the availability of a patch, accesses and downloads the patch and installs the same on the computer system.
- "a security system memory which contains security information for performing the analysis of the computer apparatus" As outlined in the functional description of the Vulnerability Scanner, [redacted] This information is [redacted] The information [redacted]

[redacted] It is at this point that the system user is given the option to decide which updates to install or otherwise. Alternatively, if the user has reconfigured the Vulnerability Scanner to automatically update software, [redacted]

- The final identified step of the security assessment is that "upon receiving an appropriate command, initiating the corrective measures." Upon display of its analysis report on its GUI, the WSS Vulnerability Scanner presents the system user with multiple options including the choice to scan the system again, selectively install discovered updates, or cancel the report. In the event the user chooses to install any or all prescribed updates, the Vulnerability Scanner carries out this task and provides a conclusive report upon completion detailing the success or failure of the update process. Alternatively, if the user has reconfigured the Vulnerability Scanner to automatically update software, the software itself issues a command to initiate the corrective measures.

**2. Dependent Claim 12**

Dependent Claim 12 identifies several types of security assessments. WSS includes "analyzing the system memory to identify system vulnerabilities." As detailed earlier, analysis of the system memory is an important step for the WSS to provide complete security for the computer system. Specifically as the Vulnerability Scanner deals with known vulnerabilities in select applications, both groups of which make very active use of the system memory, the need for the WSS to continuously analyze the system memory is crucial.